Cyber, Cyber - Krieg und Frieden in einer vernetzten Welt

Thiel, Thorsten

Postprint / Postprint
Zeitschriftenartikel / journal article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Hessische Stiftung Friedens- und Konfliktforschung (HSFK)

Empfohlene Zitierung / Suggested Citation:
Thiel, T. (2015). Cyber, Cyber - Krieg und Frieden in einer vernetzten Welt. *Polar : Politik, Theorie, Alltag*, 19, 55-61. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54916-6

Cyber, Cyber – Krieg und Frieden in einer vernetzten Welt

Thorsten Thiel

Cyberwar hat in der letzten Dekade eine immer breitere politische und mediale Aufmerksamkeit erfahren. Die digitale Infrastruktur moderner Gesellschaften gilt als hochkomplex und nur von wenigen verstanden, die Angewiesenheit moderner Gesellschaften auf sie zugleich aber als absolut. Die nahezu vollständige Digitalisierung unserer Wissensbestände und die Vernetzung des Alltags erzeugen insofern nicht nur Produktivität und Bequemlichkeit, sondern gewissermaßen als ein Nebenprodukt auch ein gesellschaftsweites Gefühl von Verletzlichkeit. *Cyberwar* – für den es bezeichnenderweise selbst in vielen deutschen Regierungsdokumenten keine deutschsprachige Entsprechung gibt – bzw. *Cyberterrorismus* – als Unterform, die von nicht-staatlichen Akteuren ausgeht – sind im Zuge dieser Entwicklung in den Rang schwerwiegender Sicherheitsbedrohungen aufgestiegen. Regierungen organisieren Abwehrmaßnahmen, private Sicherheitsdienste prosperieren und in den Medien wird regelmäßig und im Tonfall größter Besorgnis über Angriffe und Schwachstellen berichtet –etwa zuletzt im Fall des Bundestags-Hacks. Auch popkulturell findet das Phänomen *Cyberwar* viel Resonanz: So unterstreicht der Film *Blackhat* von Michael Mann, in der Ästhetik von Katastrophenfilmen gedreht, die globale Hilflosigkeit gegen die Gefahren aus dem Netz, oder der letzte James Bond *Skyfall* illustriert die arbiträre Macht jener, die die digitale Sphäre beherrschen, indem mittels digitaler Wunderwaffen auf Knopfdruck Explosionen irgendwo im Stadtbild von London auslösbar werden. Die Furcht vor einem digitalen „Pearl Harbour", so der ehemalige amerikanische Verteidigungsminister Leon E. Panetta, ist groß. Das gegenwärtige Aufbrechen geopolitischer Rivalitäten bildet zudem eine wirksame Hintergrundfolie dafür, Ängste vor dem Krieg aus dem Netz zu schüren.

Schon eine lose Aufzählung von gemeinhin mit dem Schlagwort *Cyberwar* umschriebenen Ereignissen zeigt jedoch, dass die Übertragung der Begrifflichkeit des Krieges in die Welt der Bits und Bytes weder einfach noch einheitlich ist. Unter *Cyberwar* wird häufig ganz umfassend und undifferenziert alles subsumiert, was man mit Computern so Bedrohliches anstellen kann. Der Ausdruck öffnet einen sehr diffusen Projektionsraum: Von der Spionage bis zur Blockade, von der Sabotage hin zum Datendiebstahl – fast alles kann als Angriff markiert und somit als der Logik des Krieges zugehörig interpretiert werden. Mit häufig bedenklichen Folgen für den Rechtsstaat und die Demokratie – etwa wenn digitaler ziviler Ungehorsam nicht nur kriminalisiert, sondern häufig sogar in den juristischen Kontext von Terrorismus- und Spionageparagraphen gestellt wird.

Das Konzept des Krieges, welches in anderen Instanzen wie dem *War on Drugs* oder dem *War on Terrorism* bereits ungemein geweitet wurde, wird mit dem *Cyberwar* noch ein weiteres Mal ausgedehnt. Klassische Merkmale des Krieges – wie physische Gewalt oder anhaltende Auseinandersetzungen – lassen sich für die bisherigen Cyberereignisse kaum feststellen. Selbst relativ klar dem Begriff zuzuordnende Ereignisse, etwa die digitalen Scharmützel am Rande des Krieges zwischen Georgien und Russland 2008 oder *Stuxnet* (der Angriff auf die iranischen Nuklearfähigkeiten, dem durch die Zerstörung der Zentrifugen sogar eine physische Komponente eigen ist), müssen eher als strategische und isolierte Aktionen betrachtet werden. Diese können einen Konflikt anheizen und taktische oder strategische Bedeutung haben, sind

jedoch eigentlich nicht sinnvoll eigenständig als Krieg zu klassifizieren. Was jedoch passiert, wenn diese Gleichsetzung erfolgt, ist, dass Cyber-Attacken zunehmend auch konventionell vergolten werden dürfen, wie sich etwa in der Verschärfung von Sanktionen gegenüber Nordkorea durch die Vereinigten Staaten zeigte, nachdem dem dortigen Regime die Verantwortung für den *Sony-Hack* zugeschrieben wurde.

Inwiefern *Cyberwar* eine reale Gefahr ist und wie er sich zu klassischen Kriegsdefinitionen, insbesondere zu der kanonischen von Clausewitz, verhält, ist ein Gegenstand hitziger akademischer Debatten. Die folgenden Überlegungen werden dies aber gar nicht vertiefen, sondern vielmehr eine Einordnung der Diskussion um den *Cyberwar* in das weitere Thema der Entwicklung des Internets und unserer Vorstellungen von diesem leisten. Meine These lautet, dass – analog zu Charles Tillys berühmten Diktum ‚States make war and war makes states' – dem Szenario vom Krieg im digitalen Raum eine nicht zu unterschätzende Bedeutung beim Aufstieg souveräner Staatlichkeit als Ordnungsprinzip im digitalen Raum zukommt. Der *Cyberwar* hat das Netz insofern schon lange vor jenem Tag verändert, an dem er überhaupt einmal stattgefunden hat. Dies macht jedoch im Umkehrschluss, und dies ist das zweite Argument des Artikels, es bereits heute wichtig, über den Gegenbegriff zum *Cyberwar*, den *Cyberpeace*, nachzudenken. Frieden im Netz meint dann nämlich nicht nur die Abwesenheit von Krieg, sondern muss mit einer anderen Ausgestaltung und Vorstellung, der uns umgebenden digitalen Infrastrukturen beginnen.

Souveräne Staatlichkeit, Krieg und der digitale Raum

Wer die Geschichte des Internets erzählt, beginnt häufig mit der Rolle, die der Staat, in Form von Wissenschaft und Militär, bei dessen Entwicklung gespielt hat. Die Genese eines sich dezentral selbstorganisierenden Netzwerkes wird dann als Reaktion auf die Gefahr einer Ausschaltung von Kommandoebenen im Fall eines nuklearen Erstschlags dargestellt. Obwohl Staaten und militärischer Nutzung insofern eine Bedeutung mit Blick auf die Entwicklung der Architektur moderner Informations- und Kommunikationstechnologien (IKT) zukommt, treten diese im Zuge der Durchsetzung digitaler Netzwerke doch weit in den Hintergrund. So sind die Jahre des digitalen Aufbruchs – zugleich die Zeit nach dem Ende des Kalten Krieges – geprägt von digitalen Utopien. In diesen wird das Internet als ein souveränitätsaverser, freiheitlicher Raum beschrieben. Die disruptive Kraft des Internets wird als Sargnagel hierarchischer Steuerung beschrieben, das Netz zu einer, wenn nicht der Symbolfigur für die unaufhaltsame Kraft der Globalisierung und die Möglichkeit umfassender und gleichberechtigter Partizipation. Die klassischen Kennzeichen und Instrumente des Staates – Gewaltmonopol, Grenzen, Recht – scheinen angesichts des freien Fluss von Kommunikationen antiquiert; neue, und scheinbar überlegene Formen der kollektiven Koordination (Governance) schicken sich an, das Erbe staatlicher Souveränität anzutreten.

Obwohl bereits diese frühen Beschreibungen eines souveränitätslosen Internets übersteigerte Projektionen einer kleinen, technikbegeisterten Elite sind und der Staat zu jedem Zeitpunkt der Entwicklung über durchaus substantielle Möglichkeiten der Regulierung digitaler Infrastruktur und Entwicklung verfügte, spielt die Vorstellung des Internets als staatenloser Raum doch eine große Rolle für dessen Entwicklung. Die Annahme alternativer Normen und Handlungslogiken diente als Motor für die Entwicklung neuer Geschäftsmodelle und einer transnational

organisierten, zivilgesellschaftlich begleiteten Verwaltung des Netzes. Diese mag zwar nicht immer so radikal anders und effizient sein, wie von ihren Befürworten behauptet – weist eventuell sogar einige schwerwiegende, auch die eigene Selbstreproduktion gefährdende architektonische Probleme auf –, sie ist jedoch als entscheidend für die rasante Ausbreitung der IKTs anzunehmen.

Doch genau dies ruft den Staat alsbald wieder auf den Plan: Das rasante Wachstum des Internets führt dazu, dass Staaten jedweder Couleur ein umfassendes und anhaltendes Interesse an der Möglichkeit zur Regulierung und Überwachung digitaler Kommunikation entwickeln. Die zunächst herrschende populäre Annahme der unregierbaren Dynamik der Netzentwicklung und der daraus abgeleitete Weg der Selbstbeschränkung und des Garanten einer freiheitlichen Entwicklung werden schnell wieder zugunsten einer Bemühens um engmaschige Kontrolle aufgegeben. Mit dem Ergebnis, dass in der Gegenwart die Organisation digitaler Netze längst nicht mehr durch die Offenheit geprägt ist, die in der Architektur der Protokolle angelegt ist oder in den Visionen der technischen *communities* der frühen Jahre dominant war.

Es ist diese Entwicklung, die durch die rhetorische Figur des *Cyberwar* und die Ausweitung des Konzepts der *Cybersicherheit* teilweise legitimiert wird. Der Verweis auf die Gefahren einer dezentral organisierten Infrastruktur leitet eine Transformation ein, die Staaten aktiv in die Rolle des Produzenten von Sicherheit setzt. Die Sprach- und Bildwelt des *Cyberwars* wird daher oft gerade durch Vertreter des Staates in den öffentlichen Diskurs eingespeist. Nachvollziehen lässt sich dies an der Umstellung von der Semantik der Computersicherheit, die auf Integrität und Konnektivität abzielt und technisch codiert ist, zur *Cybersicherheit*, die auf diffuse Werte und Infrastrukturen abstellt und sich nicht mehr lokal verwirklichen lässt. Verantwortung für das Netz wird so auf Staatlichkeit hin ausgerichtet, zudem zwischen online und offline vermischt. Nationale bzw. regionale Institutionen entstehen, die speziell und in einem militärischen Duktus auf die Erzeugung von Sicherheit gerichtet sind – etwa das beim BMI angesiedelte deutsche nationale Cyber-Abwehrzentrum oder das NATO Cyber-Defence-Centre in Talinn. In die Öffentlichkeit treten diese Institutionen dann hauptsächlich durch die Simulation von Ernstfällen, welche wiederum das Bewusstsein der Gefahren schaffen und den Respekt vor den staatlichen Kapazitäten zu schärfen suchen.

Eine zentrale Eigenschaft des neuen Sicherheitsdiskurses ist dessen selbstverstärkende Wirkung. Die Aufrüstung der Staaten im Netz führt geradewegs in eine Aufrüstungsspirale, für die weder eine Selbstbegrenzung zu erwarten ist noch der mit einer diplomatischen Einhegung zu begegnen wäre. Dies liegt unter anderem daran, dass mit Blick auf digitale Sicherheitsproduktion offensive Kapazitäten als herausragend wichtig erachtet werden. Dies wird mit Attributionsproblemen, knappen Zeithorizonten und der Gefahr asymmetrischer Angriffe begründet. Ein Fokus auf Offensivpotentialen aber führt nahezu zwangsläufig in die als überkommen angenommene Logik der Abschreckung. Ein globales Wettrüsten im digitalen Raum ist die Folge.

Flankiert wird dies, durch den Ausbau umfassender Kapazitäten zur Überwachung digitaler Kommunikation. Diese Seite des Cyberdiskurses ist insbesondere durch die Snowden-Enthüllungen in das Bewusstsein der Öffentlichkeit getreten, wobei das Argument, dass Prävention und umfassende Kontrolle die einzig mögliche Strategie in einem durch Digitalisierung verdichteten Raum sei, selbst durch die Politisierung der Debatte nicht gebrochen

werden konnte. Auch liberale, demokratische Staaten halten an dem Versicherheitlichungsdiskurs entschieden fest; ja, sie sind gar treibende Kräfte in ihm.

Insgesamt mündet diese Entwicklung darin, dass unsere Vorstellung vom Internet heute nur noch partiell auf die Netzwerklogik verstreuter und flexibel verbundener Akteure verweist, hingegen mehr und mehr kompatibel geworden ist, mit der Freund-Feind-Logik in der sich klassische Souveränität und Staatlichkeit ausdrücken lässt. Die optimistischen Prognosen vom Rückzug oder der Transformation von Staat und Staatlichkeit im und durch das Netz sind daher gerade in jenem Segment hinfällig, in dem der Staat nie eine Rolle zu spielen schien. Vielmehr drängen Staaten gerade in der digitalen Dimension ganz klassisch auf die Entwicklung eines Gewaltmonopols und etablieren eine umfassende Fürsorgepflicht. Dass dabei ein Wettkampf um digitale Superiorität und Hegemonie entsteht, der Balkanisierungstendenzen (die chinesische und russische Abschottung der eigenen Netzinfrastruktur und -kommunikation) und Hegemonialkämpfe (das Gebaren westlicher Geheimdienste) befördert, ist eine paradoxe und tatsächlich die Sicherheit im Netz umfassend unterminierende Wirkung.

Make Love, not War: *Cyberpeace* als diskursive Transformation

Dies bringt mich abschließend zu der Frage, wie wir *Cyberpeace* verstehen können und sollten. Die Diskussion hierüber ist noch jung und wenig spezifisch. In ihr zeigt sich, dass das *Fearmongering* der Staaten die zwar virulente, oft jedoch um die eigenen Themen und Lebenswelten kreisende netzpolitische Community lange nicht zu tangieren schien. In den letzten Jahren, und natürlich nochmal verstärkt durch die Enthüllungen über die Überwachungspraktiken westlicher Geheimdienste, haben sich aber zunehmend Initiativen gebildet, die bewusst versuchen, technische, politische und rhetorische Abrüstung voranzutreiben – etwa die Kampagne *Cyberpeace* (http://cyberpeace.fiff.de/), die vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. betrieben wird.

Da *Cyberwar* real ist, solange wir an ihn glauben und für ihn rüsten, kann es bei *Cyberpeace* nicht einfach nur darum gehen, Staaten zu Friedfertigkeit anzuhalten und unmittelbare Konflikte zu schlichten. Es bedarf vielmehr einer mehrdimensionalen Strategie:

Die erste Dimension sollte an den Bedingungen der Möglichkeit von sicherer Kommunikation in digitalen Netzwerken ansetzen. Es ist ja tatsächlich so, dass die enorme Bedeutung digitaler Kommunikation, die Steuerung technischer Anlagen und die Angewiesenheit von Öffentlichkeit, Ökonomie und Verwaltung auf digitale Prozesse dazu führen muss, dass Sicherheitsstandards fest in unserer digitalen Infrastruktur verankert werden. Die Protokolle und Standards, auf denen unsere heutige Vernetzung aufruht, sind oftmals in einer Zeit definiert worden, wo die jetzigen Einsatzgebiete unvorstellbar und die Ressourcen ungemein knapp waren. Kollektive Ressourcen – seien sie staatlicher oder privater Natur – müssten daher weit stärker dafür eingesetzt werden, den Unterbau unserer digitalen Kommunikation zu prüfen und ggf. zu renovieren. Der Fokus hier muss aber auf Computersicherheit und damit der Verteidigung/Integrität der Systeme liegen. Anstatt Schwächen ausfindig zu machen, um diese für potentielle Angriffe zu markieren, sollte Verschlüsselung und Anonymität politisch, rechtlich und technisch durchgesetzt und gestärkt werden.

Als zweites muss die Entwicklung gemeinsamer freiheitlicher und friedlicher Normen sowie der mit deren deren Durchsetzung beauftragten globalen Institutionen vorangetrieben werden. Der Einsatz für ein offenes Internet ist zwar formal schon lange Teil westlicher Staatsräson, allerdings ist dies – nicht zu Unrecht – oft als allein strategisches Element wahrgenommen worden. Hinter der Forderung nach einer Öffnung der Netze versteckte sich oft ein marktliberaler Imperativ oder politische Interessen. Die Wahrnehmung dieser doppelzüngigen Politik und die fortgesetzte Verletzung der Standards durch den Westen selbst, hat die Integrität des emergenten Normgeflechts nachhaltig beschädigt. Offene Widersprüche, wie der Verkauf von Zensursoftware, eigene Internetfilterung durch westliche Staaten oder das Agieren westlicher Geheimdienste, haben die Vertrauensbasis weltweit erodieren lassen. Die Institutionen der *Internet Governance* haben sich zudem jenseits technischer Fragen weder als sonderlich inklusiv noch als durchsetzungsfähig erwiesen. Während es für eine Reform der politischen und rechtlichen Struktur eines transnationalen Netzraums insofern keine erfolgsversprechende Blaupause gibt, so ist doch sehr klar, dass es ohne ein umfassendes Bekenntnis zu einem offenen und globalen Internet nicht gehen wird. Das nachweisliche und bestimmte Zurückfahren der Überwachungsinfrastruktur wäre ein erster Schritt, um überhaupt wieder Vertrauen aufbauen zu können.

Drittens schließlich – und analog zu dem oben gemachten Punkt, dass der *Cyberwar* zumindest auch ein rhetorisches Konstrukt ist, bedarf es eines zivilgesellschaftlichen Einsatzes für ein anderes Internet. Dieses muss die Utopie eines offenen, multifunktionalen Netzwerks wieder selbstbewusst im öffentlichen Diskurs propagieren und sowohl der staatlichen Deutung als Gefahrenraum wie der kommerziellen Deutung einer rund um die Uhr geöffneten Mall eine attraktive Vorstellung entgegensetzen. Den offenen Kommunikationshorizont als Chance für Freiheit und damit Frieden zu begreifen, bedeutet, in diesem den eigentlichen und besten Schutz demokratischer Prozesse zu verstehen. Zwar kann Offenheit nicht behaupten, sämtliche Risiken zu eliminieren – wie es sicherheitsbasierte Ansätze versprechen und doch nie einzuholen vermögen –, sie kann aber de facto eine hohe Resilienz erzeugen und aus sich heraus Dynamiken hervorbringen, die verhindern, dass das Internet den Weg anderer Kommunikationsmedien geht, die nach einer Phase der offene, kreativen Strukturgebung, sich über Zeit in geschlossene, völlig vermachtete Blöcke verwandelten.